Federal Communications Commission Notice of Proposed Rulemaking
CC Docket No. 96-115

This comment is offered in response to the Federal Communication Commission (FCC) Notice of Proposed Rulemaking to further protect the privacy of customer proprietary network information (CPNI) that is collected and held by telecommunications carriers.[1] I am pleased to be able to respond to the FCC's invitation, and I offer an evaluation of the FCC's proposal on the overall impact of any FCC rulemaking on consumer welfare without representing the views of any particular affected party or special interest group.

Introduction

The FCC should be commended for opening this proceeding to identify and to prevent the unauthorized disclosure of CPNI.[2] Granting the petition for rulemaking filed by the Electronic Privacy Information Center (EPIC) was appropriate given the concerns about whether telecommunications carriers are adequately protecting customer call records, but EPIC has overstated the value to consumers of imposing enhanced security and authentication standards on wireless carriers. Agency imposed regulations are neither necessary nor warranted at this time.

---

[1] Notice of Proposed Rulemaking (NPRM), CC Docket No. 96-115 and RM-11277, FCC 06-10, Customer Proprietary Network Information, 71 Fed. Reg. 13317 (proposed Mar. 15, 2006) [hereinafter Notice].

[2] Section 222 of the Communication Act of 1934 established a telecommunications carrier's duty to protect the confidentiality of CPNI. 47 U.S.C. § 222 (2000).

The Telecommunications Act of 1996 (1996 Act) became law on February 8, 1996.[3] Congress' intent for the Act was to "provide for a pro-competitive, de-regulatory national policy framework designed to accelerate rapidly private sector deployment of advanced telecommunications."[4] However, § 222 was included to prevent consumer privacy protections from being inadvertently swept away along with the prior limits on competition.[5] In § 222, Congress laid out a framework for carriers' use of customer information based on the sensitivity of the information. Congress accords CPNI - which includes personal, individually identifiable information - the greatest level of protection.[6] This section goes on to define CPNI as:

> (A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and
> (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier.[7]

CPNI includes highly-sensitive personal information such as the phone

---

[3] Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (1996 Act); codified at 47 U.S.C. §§ 151 et seq.

[4] Joint Statement of Managers, S. CONF. REP. NO. 104-230, 104th Cong., 2d Sess., 1 (1996).

[5] *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information and Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as amended*, CC Docket Nos. 96-115 and 96-149, Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061, 8064, ¶ 1. (1998) [hereinafter CPNI Order].

[6] U.S. West, Inc. v. F.C.C., 182 F.3d 1224, 1229 (1999) ("Given the sensitive nature of some CPNI, such as when, where, and to whom a customer places calls, Congress afforded CPNI the highest level of privacy protection under § 222.").

[7] 47 U.S.C. § 222(h)(1) (2000).

numbers called by a consumer; the frequency, duration, and timing of such calls; and any services purchased by the consumer, such as call waiting.[8] This personal information is meant to be shared with the customer, but otherwise protected unless the customer consents to any disclosure. At the customer's direction § 222 guarantees that customers have the right to obtain access to, and to compel disclosure of, their own CPNI.[9] On February 26, 1998, the FCC released the *CPNI Order* in which it adopted a comprehensive set of rules implementing § 222.[10] Consistent with § 222(c)(2), the FCC *CPNI Order* recognized that a carrier must comply with the express desire of a customer seeking the disclosure of his or her CPNI.[11] In order to implement these requirements by the FCC, telecommunications carriers must train their personnel as to when they are and are not authorized to use or to disclose CPNI, including putting into place express employee disciplinary processes for any violations.[12] Telecommunications carriers must walk a thin line between meeting their obligation to offer customer access to CPNI while protecting CPNI from all the rest of the world.

The FCC safeguard rules also require carriers to maintain records that track access to customer CPNI records. Specifically, section 64.2009(c) of the FCC's rules

---

[8] Notice, *supra* note 1, at 3.

[9] *See* CPNI Order, 13 FCC Rcd at 8101-02, para. 53.

[10] CPNI Order, 13 FCC Rcd 8061.

[11] 47 U.S.C. § 222(c)(2); *see also, e.g.*, CPNI Order, 13 FCC Rcd at 8101-02, para. 53; 47 C.F.R. § 2005(b)(3) (2005) (prohibiting the disclosure of CPNI without opt-in consent except as permitted by section 222 of the Act or the Commission's rules).

[12] 47 C.F.R. § 64.2009(b) (2005); *see also* CPNI Order, 13 FCC Rcd at 8198, para. 198.

require carriers to "maintain a record of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI," and to maintain such records for a period of at least one year.[13] In addition to this record, the FCC requires each carrier to file a certification with the FCC annually regarding its compliance with the carrier's CPNI requirements and to make this certification publicly available.[14]

In the past, much attention has been paid to the issue of open disclosure to consumers and proper use of CPNI by telecommunications carriers for marketing and other purposes.[15] The current threat to CPNI arises from the unauthorized disclosure to third parties outside the carrier-customer relationship. Recent publicity concerns the activities of online data brokers, which offer to obtain and sell individuals' wireless telephone billing and call detail records.[16] The ability of these

---

[13] 47 C.F.R. § 64.2009(c); *see also* CPNI Order, 13 FCC Rcd at 8198-99, para. 199.

[14] 47 C.F.R. § 64.2009(3); *see also Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information and Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as amended*, CC Docket Nos. 96-115 and 96-149, Order on Reconsideration and Petitions for Forbearance, 14 FCC Rcd 14409, 14468 n.331 (1999) (clarifying that carriers must "make these certifications available for public inspection, copying and/or printing at any time during regular business hours at a centrally located business office of the carrier"). The Commission's rules also require carriers to notify the Commission in writing within five business days of any instance in which the opt-out mechanisms did not work properly, to such a degree that consumers' inability to opt-out is more than an anomaly. 47 C.F.R. § 64.2009(f); *see* Third Report and Order, 17 FCC Rcd 14860, 14910-11, paras. 114-15 (2002) (adopting such requirement).

[15] *See* Leah E. Capritta, *Communications Law: U.S. West, Inc. v. FCC Interprets the First Amendment Ramifications of "Customer Proprietary Network Information*, 77 DENV. U. L. REV. 441, 442-46 (2000); Safeguards Required for Use of Customer Proprietary Network Information, 47 C.F.R. § 64.2009 (2005).

[16] Charles Kennedy, *Illicit Data Brokers Draw Response from Congress, FCC, and Mobile Carriers*, COMMUNICATIONS LAW BULLETIN - JANUARY 2006, Feb. 20, 2006.

data brokers to obtain private phone records has been widely reported.[17] Whether these records are being obtained through the process of pretexting, hacking into company records, or merely by paying employees to defeat the internal security precautions, the issue has risen to the forefront of the privacy debate in this country. Pretexting, as a fraudulent practice, is designed specifically to obtain a customer's personalized information through illegitimate means.[18]

The principle issue in this proceeding involves defining what agency measures should be put into place in light of the increasing danger presented by the unauthorized disclosure of CPNI. The five proposed safeguards offered by EPIC as a means to prevent future CPNI breaches are: 1) consumer-set passwords, 2) audit trails, 3) encryption, 4) limiting data retention, and 5) notice and reporting. Like the regulatory actions taken by the FCC in the past to implement the protections granted by the Telecommunications Act, the FCC has the authority to take the actions suggested by EPIC. However, the FCC must consider whether action at this time is appropriate under the current legislative climate sweeping the country in response to this threat to personal information security. The FCC could best promote privacy and security interests by taking the following steps:

---

[17] *See* Karen Johnson, *Firms Selling Phone Data are Targeted Senate Passes Bill Online Companies Peddle Information About Users' Calls*, SEATTLE TIMES, Feb. 18, 2006 (crediting the attention over online data brokers to the national attention directed at Washington, D.C., blogger John Aravosis when he claimed to buy the cellphone records of former presidential candidate Gen. Wesley Clark with an $89.95 credit-card payment); Charles H. Kennedy, *Fallout from Pretexting Incidents Continues*, COMMUNICATIONS LAW BULLETIN – FEBRUARY 2006, Mar. 3, 2006, *available at* http://www.mondaq.com/i_article.asp_Q_articleid_E_38106 (noting the "particular prominence by press disclosures" of the problem of pretexting).

[18] The FCC has identified pretexters as those who obtain CPNI by posing as the customer, and then offering the records for sale on the Internet. FCC Press Release, FCC Examines Need for Tougher Privacy Rules: Comment Sought On Measures Proposed by EPIC (Feb. 10, 2006).

1) Declare unreasonable any specific guidelines or national standard that restrict the ability of wireless carriers to develop unique and flexible security measures to counter any new methods of unauthorized disclosure developed by fraudulent third parties over time.

2) Impose reporting requirements on telecommunications carriers for any breach of existing security measures, including the nature and extent of the security failure in order to inform the public and other industry participants. This would include simplifying the certification requirements for telecommunications carriers to ensure that the information is made more accessible to the public, which includes other carriers so that each can learn from the others' mistakes.

I. The Importance of Protecting CPNI is Not in Dispute

There is a growing public recognition that the misuse of personal data is harmful.[19] The misuse of personal information is both a personal wrong to individuals and a public wrong to society.[20] With the rise of identity theft, the public is concerned about the safety of personal information.[21] However, identity

[19] Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877, 884 (2004).

[20] *Id.* at 896.

[21] 27.3 million Americans have been the victim of identity theft in the past five years, costing businesses and financial institutions approximately $48 billion annually and consumers $5 billion. *Oversight Hearing on Data Security, Data Breach Notices, Privacy and Identity Theft Before the Committee on Banking, Housing and Urban Affairs* 5 (2005) (statement of Edmund Mierzwinski, U.S. PIRG Consumer Program Director).

theft is not the only possible negative consequence of unauthorized disclosure of CPNI. Dissemination of CPNI is not only an invasion of privacy, but such breaches also compromise personal safety, especially with regards to the victims of domestic violence and other crimes.

The concerns of various domestic violence coalitions that illegal access to these consumer records can be used to track and terrorize victims cannot be disregarded lightly. EPIC suggests that CPNI may be abused in the same manner as what occurred in the *Remsburg v. Docusearch* case.[22] However, the resolution of that case held the information brokers accountable for the sale of the information, and not the source that improperly disclosed the information.[23] Liability for the sale of phone records should be equally confined to the wrongdoers like data brokers that engage in the fraudulent acts that lead to such disclosures. As there are no known legitimate methods of obtaining this information that does not involve fraud, misrepresentations or some other violation, the perpetrators of these illegitimate methods are the ones responsible for creating this threat to consumer privacy, and measures should be taken to pursue these individuals.

Law enforcement has had difficulty tracking down fraudsters in many different contexts, and there is no doubt that enforcement actions will be difficult to bring against pre-texters that are able to hide in the anonymity that the Internet

---

[22] Complaint and Request for Injunction, Investigation and for Other Relief, In the Matter of Intelligent e-Commerce, Inc. para. 7 (filed with the FTC July 7, 2005) (citing Remsburg v. Docusearch, 816 A.2d 1001 (N.H. 2003) (describing a case in which the use of brokered information enabled a stalker to locate and murder a young woman)).

[23] *Remsburg*, 816 A.2d at 1011.

provides. EPIC is correct in asserting that, "Communications carriers should be the first line of defense against these practices."[24] However, the EPIC solution of imposing on carriers a rulemaking containing industry wide security measures would hamper rather than assist current industry efforts to address this problem. When a problem exists, agency action is not always the solution. Sometimes an industry, such as telecommunications, must accommodate various competing interests at once and find individualized solutions to the problems that arise.

II. Security Interests v. Information Interests

Though the Telecommunications Act requires that carriers protect the CPNI of their customers, it also requires that it disclose such information to those same customers without undue burden or delay. Any increase in the security measures put into place should not be so overly complicated or cumbersome that it prevents or inconveniences customers from obtaining their own confidential account information.

EPIC concedes that the actions of online data brokers are illegitimate, but EPIC places the blame for these violations on the loopholes contained in the security measures of the different telecommunications carriers.[25] In their petition, EPIC suggests that telephone call records are being obtained through either

[24] Letter from EPIC to the FTC, Update to the FCC, Re: Online Data Brokers / Request for Industry-Wide Investigation (Aug. 30, 2005).

[25] Petition of the Electronic Privacy Information Center for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information before the FCC, CC Docket No. 96-115 (Aug. 30, 2005).

pretexting or insider solicitation,[26] but none of the security measures recommended by EPIC would address how to resolve the problem of insider solicitation. Understandably EPIC focuses on pretexting, since pretexting is the most common form of unauthorized access.[27] Therefore, common sense suggests that countering this particular abuse must be an obtainable goal of any regulatory action to be taken. Problematically, preventing pretexting would require more and more steps to be implemented at many levels by the telecommunications carriers, hoops to be jumped through by the customer, and other inconveniences which would ultimately all be passed onto customers in any efforts to prevail against impersonators and others fraudulent actors.

Currently, the successful data broker must identify the loopholes in the security system of each separate carrier. Under a uniform system established by the FCC, each data broker would have a regulatory roadmap to identify any loopholes that will be overlooked by the drafters of any future rule. Further, each telecommunications carrier would be forced to comply with rigid and inflexible security procedures rather than developing a more efficient and individualized security system that would reduce the cost and inconvenience to customers to both store CPNI and make CPNI available to customers on demand. Market forces provide the proper incentives for telecommunications carriers to further customer

---

[26] *Id.*

[27] The Cellular Telecommunications & Internet Association (CTIA) testified before Congress that "[o]verwhelmingly, the vast majority of cell phone records are being fraudulently obtained through the use of 'pretexting.'" *See* Letter from Paul Garnett to Marlene H. Dortch, Secretary, FCC, CC Docket No. 96-115 Attach. at 2 (filed Feb. 2, 2006).

interests in protecting and accessing CPNI without any additional interference by the FCC.

III. Market Forces would be Superior to a Regulatory Solution to Protect CPNI

Current market forces exist to provide the proper incentives for carriers to meet consumer demands to protect CPNI. Online data brokers got national attention earlier this year when Washington, D.C., blogger John Aravosis said he bought the cell phone records of former presidential candidate General Wesley Clark with an $89.95 credit-card payment.[28] And although the publicity focused on the celebrity names revealed on Paris Hilton's personal cell phone last year, the incident was a part of a larger hacker attack on T-Mobile's servers.[29] These public displays of how vulnerable personal phone records can be incited widespread concern among consumers over the security of their private information.

As the protection of CPNI is driven to the forefront of consumer awareness, the response by wireless carriers must respond to those concerns and those carriers will act appropriately to protect that information or else risk the loss of consumers. Wireless carriers exist in a highly competitive world, where their products can be swiftly evaluated by consumers, and those customers can express dislike with those

---

[28] Frank Main, *Blogger buys presidential candidate's call list: 'Nobody's records are untouchable,' as $90 purchase online shows*, CHIC. SUN TIMES, Jan. 13, 2006. *See also Call-Records Scandal Mushrooms Amid Legislative, Regulatory Fallout*, Telecom Pol'y Rep., Feb. 6, 2006, *available at* 2006 WLNR 2072663.

[29] Simple Mobile Security for Paris Hilton!, PC MAGAZINE, Mar. 1, 2005, *available at* 2005 WLNR 3834800.

products by switching carriers.[30] The ability to shift expenditures onto the providers imposes on each wireless carrier a rigorous discipline to satisfy consumer preferences with regards to CPNI.[31]

Take for example, developments in the financial market. The circumstances leading up to and following the massive security breach at ChoicePoint provides a clear picture of the motivations driving telecommunications carriers in their private efforts to prevent any unauthorized disclosures of customer information.[32] ChoicePoint has become the poster child of security breaches concerning consumer information, and the recent history of this company sets forth a tale of warning to other industries to protect such information or face the media firestorm and public backlash that followed the 2005 security breach. Today, ChoicePoint has implemented new security measures along with other financial institutions following in its stead. These measures are not altruistic in nature, but the a response to the reality of competing in an industry that requires security of customer information.[33] Many other different industries have been the victim of

---

[30] The ability to "punish" wireless carriers for not satisfying customer preferences has only increased with the introduction of wireless local number portability. *Telephone Number Portability*, Third Report and Order, CC Docket No. 95-116, 13 FCC Red 11701 (1998).

[31] Timothy J. Muris, *The Federal Trade Commission and the Future Development of U.S. Consumer Protection Policy* 6 (unpublished manuscript), *available at* http://ssrn.com/abstract_id=545182.

[32] ChoicePoint, a Georgia-based data broker, acknowledged it had inadvertently sold personal information about 145,000 consumers to a suspected criminal ring. Bill Swindell, *Committee Changes In ID Theft Measure Draw Fire From Business And Consumers*, CONGRESS DAILY, Feb. 10, 2006.

[33] Bill Husted, *ChoicePoint's recovery: A Year After Embarrassing Security Breach, Data Broker has Changed its Ways, Grown its Business and Silenced Some Critics*, ATLANTA JOURNAL AND CONSTITUTION, Feb. 12, 2006 (citing Larry Ponemon, a part of the information security group called the Ponemon Institute (""It's not because of altruism. . . . They can't afford to have a brand meltdown over this again.")).

security breaches in the past year,[34] and no doubt none of the current major telecommunications carriers are eager to be the first wireless company to appear in the headlines with a major security breach.

Statutes such as the Telecommunications Act cannot address the full set of concerns associated with privacy, and tort protections have not expanded to fill the statutory voids and deal with the significant conceptual obstacles to security.[35] Whatever form of unauthorized disclosure is currently taking place, through pretexting or some other means, these methods will not the last, and others are certain to be developed by wrongdoers in the future. These gaps in the scope of any statutory language can only be filled through the marketplace and alternative forms of policing.[36] Rather than taking regulatory action, the FCC must encourage carriers to seek out the most innovate products and services when implementing security measures rather than establishing a minimum bar of safety or restricting carriers to conform to a set of security guidelines. Telecommunications carriers

---

[34] *See* Renita Fennick, *Debit-card Security Addressed*, TIMES LEADER, Mar. 11, 2006 (reporting security breaches at PNC and Citizens Bank); *Times Co. Papers Slip Up on Credit Card Data*, NEWSDAY, Feb. 1, 2006 (reporting two newspapers that had mistakenly sent out slips of paper with the credit card data of up to nearly a quarter million subscribers); Dan Caterinicchia, *New State Laws Seek to Halt Identity Theft: Similar Federal Legislation Could Work Against Industry, Consumers*, WASHINGTON TIMES, Jan. 4, 2006 (reporting a security breach at Marriott Vacation Club International, Bank of America Corp., and shoe retailer DSW Inc.); Jon Swartz, *Cybercrime Hike Raises Identity Theft Worries: This Month, Several Companies Reported Computer Breaches*, CHIC. SUN TIMES, Dec. 29, 2005 (describing 2005 as the worst year for known computer-security breaches and reporting additional security breaches in the month of December at Ford Motor, ABN Amro Mortgage Group and Sam's Club).

[35] Reidenberg, *supra* note 19, at 881.

[36] *Id.*

need the freedom to be able to change existing policies to adapt to the changing nature of criminal activity.[37]

It is even possible that an FCC rulemaking would assist rather than prevent future breaches of CPNI. Set procedures and guidelines provide potential violators a virtual "roadmap" to find weaknesses in a security system. By imposing those procedures and guidelines on any company engaged in the telecommunications industry, the CPNI of each customer of all those different companies is exposed to the same level of risk. Agency mandated consumer protection measures can create barriers that limit the freedom of wireless carriers to provide the security that consumers demand.[38] Carriers should be allowed to focus their scarce resources on actually preventing those wrongdoers from perpetrating the harm rather than being forced to expend increasing amounts of money to comply with perfunctory administrative costs. By diverting resources from developing more effective security measures, wireless carriers will be more vulnerable to security breaches.

With threats looming everywhere, settling for bare minimum-security standards is not an option. The American legal system has generally rejected legal rights for data privacy and relies instead on market self-regulation and the litigation process to establish norms of appropriate behavior in society.[39] The market would inevitably serve the same function under these circumstances and

---

[37] Jonathan Krim, *Online Data Gets Personal: Cell Phone Records for Sale*, WASHINGTON POST, July 13, 2005 (quoting Jeffrey Nelson, a Verizon Wireless company spokesman as saying, "we have historically, and will continue to, change policies to reflect the changing nature of criminal activity").

[38] Muris, *supra* note 31, at 20.

[39] Reidenberg, *supra* note 19, at 877.

lead telecommunications carriers to security solutions that would be far superior than any rigidly formulated agency solution.

IV. Reporting Requirements

In order to monitor the progress that could be achieved under a market-based approach to securing CPNI, implementing reporting requirements on the telecommunications industry would serve the purpose of ensuring private action is being taken as well as creating a public resource to the benefit of consumers and other industry participants. Current rules require carriers to certify compliance with the FCC's existing CPNI rules and make that certification available to the public, but the FCC observes that a lack of uniformity in these certifications could be an obstacle to effective enforcement.[40]

When the structure for the treatment of personal information is increasingly defined through scandals and enforcement actions, it would be preferable to have a system which can self-generate sensible fair information practices.[41] The telecommunications industry leaders could work together to address this problem and develop the best and most uniform reporting system rather than having the FCC craft one through government intervention.[42] Working with the telecommunications agency to find a proper solution through reporting would be

---

[40] FCC Press Release, FCC Examines Need for Tougher Privacy Rules: Comment Sought On Measures Proposed by EPIC (Feb. 10, 2006).

[41] Reidenberg, *supra* note 19, at 884.

[42] Such a move would reflect similar action taken by the major credit reporting agencies, Equifax, Experian, and TransUnion, to voluntarily come up with an encryption standard all would use to protect sensitive customer data. *Credit Companies Promise Tighter Security*, TECHWEBNEWS, Sept. 26, 2005, *available at* 2005 WLNR 15198289.

more effective than imposing on the industry in any other ways. Further, placing additional reporting requirements on the telecommunications carriers may not be ill-received by the industry, since already there is nearly national voluntary compliance with a recent California law, which requires companies to notify state residents when their unencrypted personal information is reasonably thought to have been compromised.[43]

One additional reporting requirement the FCC should consider would be to have all the telecommunications carriers submit to the FCC each year, along with their certifications, a detailed record of any consumer complaints during the previous year on the unauthorized release of CPNI, and a summary of any actions taken against data brokers. The actions taken should include details of how the information was obtained. By identifying the newest method of data breach and placing that information on the public record, other wireless carriers can preemptively address any similar loopholes in their own security system.

Importantly, no telecommunications carrier should be required to report the internal solution developed by the carrier to resolve the security issue. In this way, no roadmap or other identifying information will be made available to wrongdoers, but the public and the other carriers will have sufficient knowledge to take independent action. The different types of threats that can be devised in the virtual environment are constantly changing, and static rules can quickly become

[43] Caterinicchia, *supra* note 34.

outmoded or easily avoided by the innovative fraudster.[44] No system can be perfectly secure considering the size of many national wireless networks, but shared information through increased reporting allows each company to stay in step with those attempting to engage in illegitimate practices.

V. Legislative Action Will Preempt the Need for an Agency Rulemaking

As technology advances, there is no way to anticipate and to counter every possible manipulation of security measures by illegal means. Carriers should not be held responsible for the illegal acts of third parties. Instead, telecommunications carriers should be empowered to take action against those third parties without being hindered by agency rules. There has been a recent flurry of legislative activity addressing this issue on both the federal and state levels. In past statements, both the FCC and the FTC, have asserted that the best way for Congress to deal with the problem of unauthorized disclosures would be to pass legislation expressly prohibiting the sale of consumers' phone records.[45] As these statutory measures are put into place, regulatory action by the agency will appear increasingly unnecessary in light of the criminal and civil devices being put into place to protect against the unauthorized disclosure of CPNI.

At least eight separate bills have been introduced in Congress during 2006 within only the last few months. For example, the Law Enforcement and Phone

---

[44] Frank Main, *FCC Subpoenas 30 Phone Record Dealers: Will Look at how They Get Call Info from Companies*, CHIC. SUN TIMES, Feb. 2, 2006 (quoting Steve Largent, president of the Cellular Telecommunication & Internet Association, cautioning against forcing carriers to employ identical security measures or to make those measures public).

[45] Dan Caterinicchia, *Sale of Phone Records Angers Lawmakers: House Hearing Focuses on Thwarting 'Pretexting'*, WASHINGTON TIMES, Feb. 2, 2006.

Privacy Protection Act of 2006 was presented in the U.S. House of Representatives,[46] and the Consumer Telephone Record Protection Act of 2006 was presented in the U.S. Senate.[47] On the state level, there have been efforts made to impose criminal penalties on the activities known as pretexting.[48] At least four states have brought suit against data brokers under these new consumer protection laws. Some consumer advocacy groups would even prefer state action over federal action, contending that many states have stronger laws than Congress is considering, and those state laws should not be preempted by any federal legislation.[49] In either respect, the criminalization of fraudulent practices to obtain CPNI is well under way, and almost certain to continue over the course of the coming year.

Another important source of legislative activity is the creation of a private right of action for the telecommunications industry to pursue violators directly. The wireless carriers generally have reaffirmed their commitment to customer privacy and have expressed their support for legislation that will criminalize the fraudulent

---

[46] H.R.4709, 109th Cong. (2006) (going before the full body of the House later this year after being approved by the House Committee on the Judiciary on Mar. 2, 2006). *See* Charlene Carter & Joelle Tessler, *HR4709 - Law Enforcement And Phone Privacy Protection Act Of 2006*, CQ BILLANALYSIS, February 15, 2006 (imposing a 20-year prison sentence and up to $500,000 penalty on anyone who sells, transfers or attempts to sell or transfer phone records without consumer authorization).

[47] S.2389, 109th Cong. (2006) (going before the full body of the Senate later this year after being approved by the Senate Committee on Commerce, Science, and Transportation on Mar. 30, 2006).

[48] The Illinois, New York, and Washington states have all passed legislation making it unlawful to engage in any of the activities known as pretexting. *See* Kennedy, *supra* note 17.

[49] "Congress doesn't need to do anything because California has solved the problem. It's being complied with nationwide," said Ed Mierzwinski, consumer program director for the U.S. Public Interest Research Group. Swindell, *supra* note 32.

activities of data brokers.[50] However, each of the five major carriers have already taken advantage of civil alternatives at their disposal and brought suit against alleged pretexters. Successes in this area of litigation concerning CPNI include obtained restraining orders and injunctions against pretexters, who the telecommunications carriers have identified as seeking to breach CPNI security procedures. T-Mobile USA Inc. obtained temporary restraining orders against two data brokers and obtained permanent injunctions against three other data brokers.[51] Sprint Nextel Corp., Verizon Communications Inc.'s Verizon Wireless, and Cingular Wireless LLC also have brought lawsuits and obtained relief against data brokers.[52] Rather than allowing the FCC to take a prescriptive approach on security that would hinder these efforts, the telecommunications carriers would support tougher enforcement of existing laws that ban the practices of data brokers. In combination with the criminal penalties, these civil sanctions serve as a deterrent on potential pretexters.

By taking actions to prevent those engaged in the practice of pre-texting and other forms of obtaining unauthorized disclosures of CPNI, these laws impose costs on those engaged in these harmful activities rather than penalizing every commercial company involved in the wireless industry. Therefore, permitting

---

[50] *FCC Starts Review Of Telephone Record Security: The move comes amid pressure to clamp down on online data brokers that offer to obtain and sell telephone subscriber information*, TECHWEBNEWS, Feb. 13, 2006, *available at* 2006 WLNR 2531786 (quoting the CTIA, the lobbying group for major wireless carriers, which has urged the FCC to avoid imposing new rules, preferring instead tough enforcement of existing laws that ban the practice).

[51] Kennedy, *supra* note 16.

[52] *Id.*

private legal rights of action against these fraudsters will be an important compliment to the market solutions that will emerge from the private sector.[53] Law enforcement efforts to enforce criminal penalties are acting in conjunction with the efforts by the telecommunications carriers to impose civil penalties against violators. The agency has no further role to play in this game of cat and mouse between enforcing the existing regulations against illegitimate data brokers.

Conclusion

In light of the legislative activity and the recent successes by the carriers in the legal context, a rulemaking that imposes further requirements is premature. The increased criminal penalties and private efforts are addressing the problem of CPNI breaches. Though there is value in attacking a problem from all sides in an "overkill" effort, it does not seem the most efficient approach. The additional burden on carriers is not justified when alternatives are available.

The goal of any FCC rulemaking on the increased security measures to be implemented by telecommunications carriers to protect CPNI would be to stop the illegitimate practices that allow data brokers to exploit private phone records. However, no such goal can be reached by implementing a uniform standard for security measures on carriers. The consumer benefits by allowing wireless carriers to develop individualized and unique security measures for CPNI. Therefore, some key steps for the FCC to initiate moving forward include:

[53] Muris, *supra* note 31, at 9.

1) Declare unreasonable any specific guidelines or national standard that restrict the ability of wireless carriers to develop unique and flexible security measures to counter any new methods of unauthorized disclosure developed by fraudulent third parties over time.

2) Impose reporting requirements on telecommunications carriers for any breach of existing security measures, including the nature and extent of the security failure in order to inform the public and other industry participants. This would include simplifying the certification requirements for telecommunications carriers to ensure that the information is made more accessible to the public, which includes other carriers so that each can learn from the others' mistakes.

CPNI may soon be at risk through other practices than pre-texting, so innovative security measures will be important in order to adapt to the changing technological climate. The FCC should be commended for bringing this proceeding to identify and prevent such practices.

Respectfully submitted,

Kim Phan
J.D. Candidate
George Mason University School of Law